Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
23 OCT 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Insider Threat Mitigation Project: A Dynamic Network Approach	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
; Carley /Andrew P. Moore KathleenClaycomb /William	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**1**	

Insider Threat Mitigation Project

A Dynamic Network Approach

CMU-CS (and CASOS):
– Dr. Kathleen Carley
– Neal Altman
– Geoff Morgan
– Matt Benigni

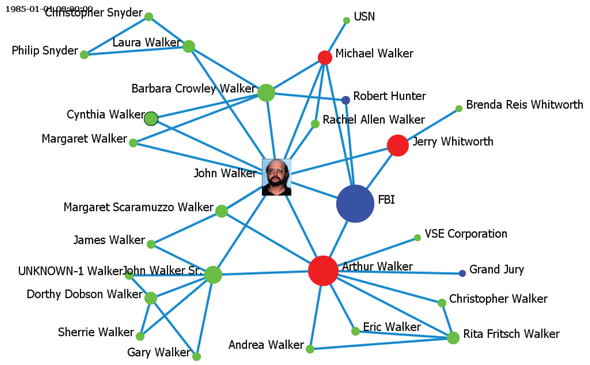
SEI:
– Matthew Collins
– Andrew Moore
– Dr. William Claycomb

Emergence of Threat – Ego centered analysis of specific cases

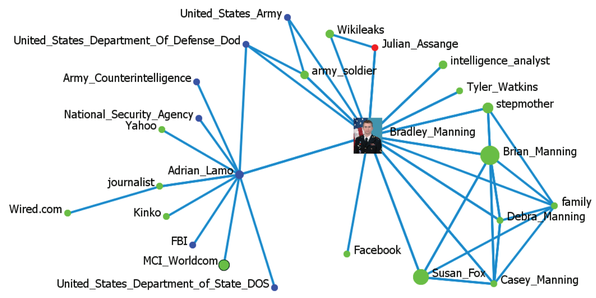
Approach:

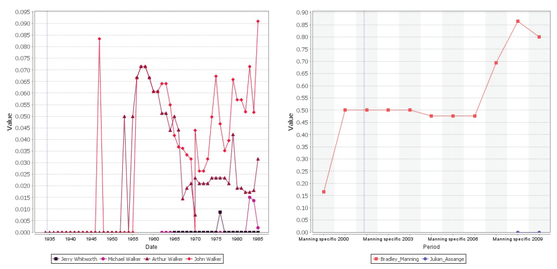
- Semi-automated coding with fine-tuning to add dates
- Extract meta-networks one per year
- Comparison at “role” level
- Apply network analytics and visualization

Walker – Gang example
Case records/searches
(open-source)

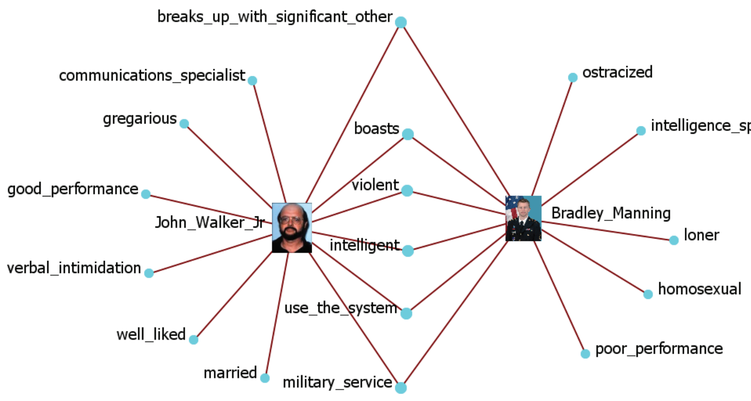


Manning – Lone Wolf
example open-source





Increasing betweenness during spy activities



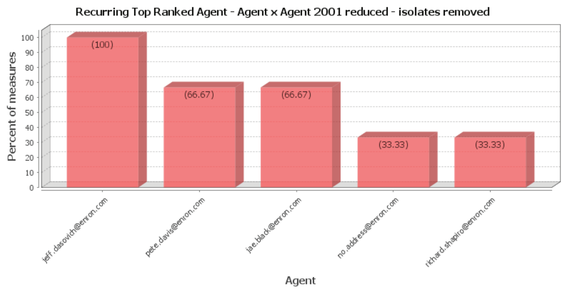
Findings on Insiders:

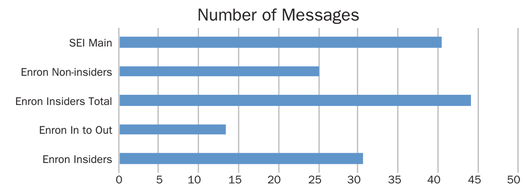
- **Special characteristics**
- **Access**
- **Increasing betweenness**
- **Disrupted family network**

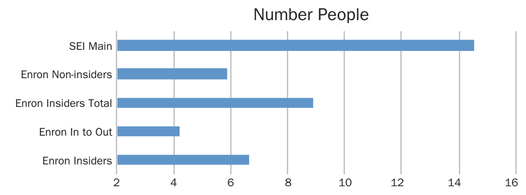
Emergence of Threat – Email centered analysis of possible anomalies

Approach:

- Networks formed from meta-data
- One network per year
- Segment internal from internal-to-external communication
- Remove suspected distribution lists
- Identify “normal behavior” using Enron
- Develop pattern for “insiders” in contrast to “normal” using Enron
- Apply to anonymized SEI email

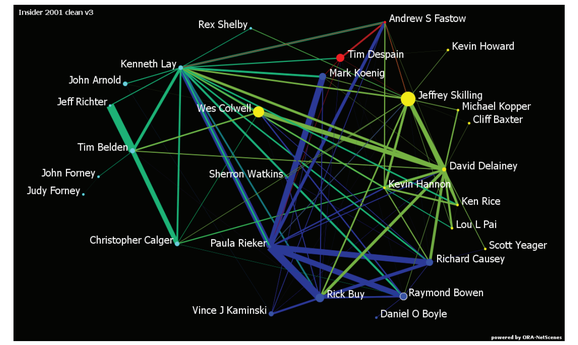




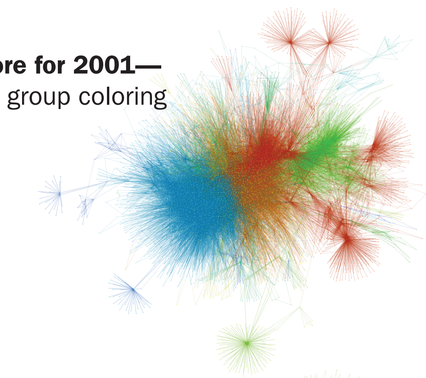


Findings on SEI -v- Enron:

- **SEI—more email, proportions similar**
- **Both—dominant dense core with numerous stars**



Enron core for 2001—
Newman group coloring



SEI core for 2013—
Newman group coloring

Findings on “Insiders”—those accused:

- **Are not “top” network actors**
- **Form a densely connected sub-group**
- **High level of in-group communication**
- **Low out-group communication**

Software Engineering Institute | Carnegie Mellon University

CASOS Center for Computational Analysis of Social and Organizational Systems

Contact: Andrew P. Moore apm@cert.org
Kathleen Carley kathleen.carley@cs.cmu.edu